(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 920 209 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.06.1999 Bulletin 1999/22

(51) Int Cl.[6]: **H04N 7/167**, H04N 7/30

(21) Application number: **98402647.6**

(22) Date of filing: **23.10.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **26.11.1997 FR 9714844**

(71) Applicant: **THOMSON multimedia**
92100 Boulogne Billancourt (FR)

(72) Inventors:
- **Pla, Véronique**
  92100 Boulogne-Billancourt (FR)
- **De Vito, Mario**
  92100 Boulogne-Billancourt (FR)
- **Fischer, Jean-Bernard**
  92100 Boulogne-Billancourt (FR)

(74) Representative:
Ruellan-Lemonnier, Brigitte et al
THOMSON multimedia,
Licensing and Intellectual Property,
46 Quai Alphonse Le Gallo
92100 Boulogne Billancourt (FR)

(54) Method and device for scrambling digital video data

(57) The invention relates to a process for scrambling video data in the MPEG2 video format as well as to a process for descrambling data scrambled according to the process of the invention.

The scrambled video data are the coefficients AC and/or DC arising from the "discrete cosine transform" operation (DCT) which are associated with at least one block of at least one image coded in INTRA mode.

The invention applies to conditional access systems such as, for example, pay television systems.

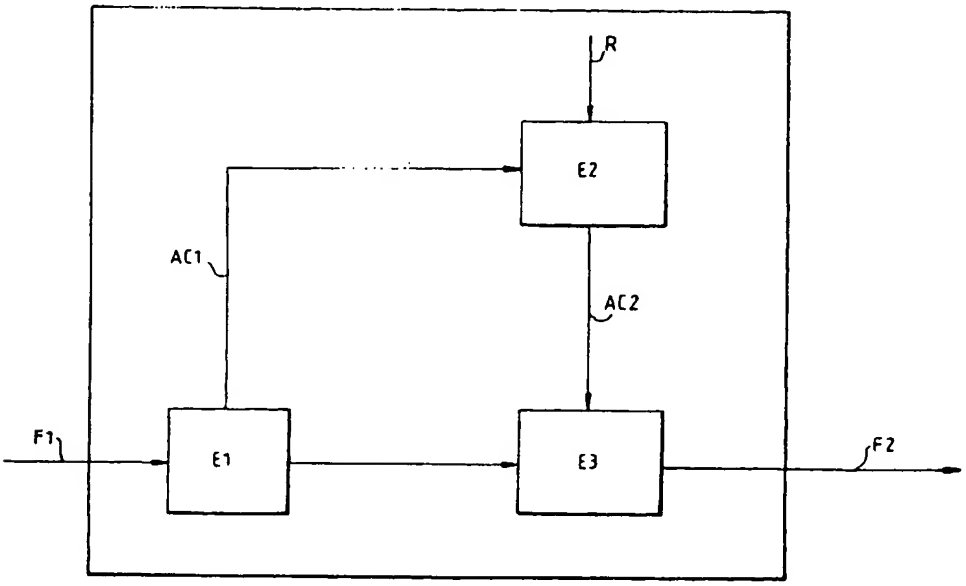

FIG.1

EP 0 920 209 A1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to a process for scrambling digital video data as well as to a process for descrambling digital video data scrambled according to the scrambling process of the invention.

[0002] The invention applies more particularly to conditional access systems for which the video data are formatted according to the MPEG2 video standard and conveyed according to the MPEG2 System transport standard.

[0003] By way of non-limiting example, a conditional access system such as the one mentioned above can be a pay television system broadcasting scrambled programmes.

[0004] As is known to the person skilled in the art, within the context of a conditional access system operating according to the MPEG2 standard, the video data are scrambled in such a way that, after scrambling, they no longer comply with the MPEG2 video standard.

[0005] In the case in which the user receiving the scrambled programme has acquired the entitlement for descrambling the programme, the scrambled video data are descrambled so as to be restored to the MPEG2 video standard. The user's MPEG2 decoder is then able to decode the descrambled video data which it receives.

[0006] In the case in which the user has not acquired the entitlement to descramble the scrambled programme, the video data are not descramble. The user's MPEG2 decoder is then totally unable to recognize the video data. No image appears on the screen: the screen is black.

[0007] The complete absence of images prevents even a glimpse of the broadcast programme and, consequently, makes it impossible to attract the attention of any potential future subscribers to the provider distributing the programmes.

[0008] The invention does not have this drawback.

[0009] Thus, the invention relates to a process for scrambling video data in the MPEG2 video format, the video data representing at least one block of at least one image coded in INTRA mode and comprising data (AC, DC) arising from a "discrete cosine transform" operation and consisting, for each block, of a first coefficient (DC) representing the mean intensity of the pixels of the block and of at least one second coefficient (AC) representing the intensity variations between pixels of the block. The scrambling of the video data is carried out by an operation for processing the data (AC, DC) arising from the "discrete cosine transform" operation compatible with the MPEG2 video standard.

[0010] The invention also relates to a process for descrambling scrambled video data, the descrambling of the video data being performed under the action of a descrambling key. The video data are data scrambled according to the abovementioned scrambling process of the invention and the descrambling key consists of at least one of the data arising from the operation for processing the data arising from the "discrete cosine transform" operation.

[0011] The invention also relates to a device for scrambling video data in the MPEG2 video format, the video data representing at least one block of at least one image coded in INTRA mode (I) and comprising data (AC, DC) arising from a "discrete cosine transform" operation and consisting, for each block, of a first coefficient (DC) representing the mean intensity of the pixels of the block and of at least one second coefficient (AC) representing the intensity variations between pixels of the block, characterized in that it comprises means for carrying out the scrambling of the video data by an operation for processing the data (AC, DC) arising from the "discrete cosine transform" operation compatible with the MPEG2 video standard.

[0012] The invention further relates to a device for descrambling video data scrambled according to the abovementioned scrambling process of the invention, the descrambling of the video data being performed under the action of a descrambling key, characterized in that it comprises means for descrambling the video data under the action of a descrambling key consisting of at least one of the data arising from the operation for processing the data arising from the "discrete cosine transform" operation.

[0013] The invention further relates to a decoder of video data coded according to the MPEG2 video standard, comprising a device for descrambling scrambled video data, characterized in that the descrambling device is a descrambling device such as the abovementioned device according to the invention.

[0014] An advantage of the invention is that it implements a process for scrambling and a process for descrambling video data which are compatible with the MPEG2 video standard.

[0015] Other characteristics and advantages of the invention will emerge on reading a preferred embodiment given with reference to the appended figures in which:

- Figure 1 represents a process for scrambling video data according to a first embodiment of the invention;
- Figure 2 represents a process for scrambling video data according to a second embodiment of the invention.

[0016] Figure 1 represents a process for scrambling video data according to a first embodiment of the invention.

[0017] The stream F1 of data which are processed according to the process of the invention comprises a succession of packets of video data coded according to the MPEG2 video standard.

[0018] The coding according to the MPEG2 video standard uses the properties of the signal to reduce the bit rate thereof.

[0019] The coding algorithm implemented describes

the images blockwise, exploiting the spatial redundancy and temporal redundancy of the images to be coded.

[0020] The spatial redundancy is evaluated, mainly, by virtue of a succession of three operations: an operation commonly referred to as "discrete cosine transform" and denoted DCT, an operation of quantizing the coefficients arising from the DCT and an operation of variable-length coding to describe the quantized coefficients arising from the DCT.

[0021] The temporal redundancy is analysed by a motion compensation operation which consists in searching, via a translation operation for each block of the current image, for the most similar block situated in a reference image. Analysis of the temporal redundancy leads to the determination of a field of translation vectors, commonly referred to as motion vectors, as well as to a prediction error which is the difference between the signal of the current image and the signal of the image predicted by motion compensation. The prediction error is then analysed according to the principle of spatial redundancy.

[0022] Coding according to the MPEG2 video standard is a coding of predictive type. It follows that the decoding procedure associated with it must be regularly reinitialized so as to protect the signal from, for example, any error of transmission or any break in signal due to the toggling of the decoder from one programme to another.

[0023] To this end, the MPEG2 video standard stipulates that, periodically, the images must be coded in spatial mode, that is to say according to a mode which exploits spatial redundancy alone. The images coded in spatial mode are commonly referred to as INTRA images or I images.

[0024] The scrambling process according to the invention is applied to the scrambling of video data corresponding to at least one block of at least one I image.

[0025] The video data which characterize an I image block contain a coefficient commonly denoted as coefficient DC (DC standing for "Direct Current") and several coefficients commonly denoted as coefficients AC (the abbreviation AC standing for "Alternating Current"). The coefficient DC represents the mean intensity of the pixels of an image block and the coefficients AC represent the intensity variations between the pixels of a block.

[0026] According to the first embodiment of the invention, for at least one block of at least one I image, the coefficients AC contained in the stream F1 and denoted AC1 in Figure 1 are extracted from the stream F1. The extraction of the coefficients AC1 from the stream F1 is represented, symbolically, by the operation E1 in Figure 1.

[0027] The coefficients AC1 extracted are then permuted amongst themselves in such a way as to constitute a new set AC2 of coefficients AC. Preferably, the various coefficients AC1 are permuted according to a permutation rank R which differs from a first set of successive blocks involved in the permutation of the coefficients AC to another set of blocks. However, the invention also relates to the case in which the permutation rank R is identical for all the successive blocks involved in the permutation of the coefficients AC. The permutation of the coefficients AC1 is represented, symbolically, by the operation E2 in Figure 1.

[0028] Following the abovementioned permutation, the coefficients AC2 are substituted, within the stream F1, for the coefficients AC1 so as to constitute the data stream F2.

[0029] The operations for extracting and permuting the coefficients AC1 as well as the operation for substituting the coefficients AC2 for the coefficients AC1 are performed, for example, by programming a microprocessor.

[0030] The data stream F2 obtained after substituting for the coefficients AC1 constitutes a stream of data scrambled according to the first embodiment of the invention. In order to constitute a data stream according to the MPEG2 System standard, the video data as scrambled are multiplexed, in a manner known per se, with audio data according to the MPEG2 audio standard and with data relating to various items of information concerning the programmes distributed.

[0031] An advantage of the invention is that it makes it possible easily to modulate the deformation of the non-descrambled images received. This is because not only can the permuting of the various coefficients AC of a block be greater or lesser, but also the number of I images on which the permuting of coefficients is performed can itself also vary.

[0032] Figure 2 represents a process for scrambling video data according to a second embodiment of the invention.

[0033] According to the embodiment represented in Figure 2, for at least one block of at least one I image, the coefficient DC contained in the stream F1 and denoted DC1 in Figure 2 is extracted from the stream F1. The extraction of the various coefficients DC1 is represented, symbolically, by the operation E4 in Figure 2.

[0034] A new coefficient DC2 is then generated, under the action of a command C, from a coefficient DC1 extracted from the stream. Preferably, the command C is a random command. The new coefficients DC2 are then substituted, within the stream F1, for the coefficients DC1.

[0035] The generating of the coefficients DC2 from the coefficients DC1 as well as the substituting of the coefficients DC2 for the coefficients DC1 within the stream F1 are represented respectively by the symbolic operations E5 and E6 in Figure 2.

[0036] The operations for extracting the coefficients DC1, for generating coefficients DC2 under the action of a command C and for substituting the coefficients DC2 generated for the coefficients DC1 are performed, for example, by microprocessor.

[0037] The data stream F3 obtained after substituting for the coefficients DC1 constitutes a scrambled data

stream. In order to constitute a data stream according to the MPEG2 System standard, the video data as scrambled are multiplexed with audio data according to the MPEG2 audio standard and with data relating to various items of information concerning the programmes distributed.

[0038] According to this second embodiment of the invention, it is also advantageously possible easily to modulate the deformation of the non-descrambled images received. This is because, here again, the larger the number of I images on which the substitutions of coefficients DC are performed, the more the image received is deformed.

[0039] Advantageously, the two scrambling processes described in Figures 1 and 2 are not exclusive of one another. Thus, a third scrambling process according to the invention relates to a process implementing both the process described in Figure 1 and the process described in Figure 2. According to this third embodiment of the invention, one and the same block for which the coefficients AC are permuted may or may not have another coefficient substituted for the coefficient DC.

[0040] As mentioned earlier, the invention relates also to a process for descrambling video data scrambled according to the scrambling process described in Figure 1 and/or the scrambling process described in Figure 2.

[0041] In order to implement the descrambling of the video data scrambled according to the process described in Figure 1, the successive permutation ranks R of the coefficients AC1 of the various blocks involved in the permutation are transmitted to the descrambling device. The successive permutation ranks R are then the keys for descrambling scrambled data.

[0042] Preferably, the successive permutation ranks R are transmitted to the descrambling device after having been encrypted according to an algorithm with key K. The transmission of the permutation ranks R is preferably performed in the stream which contains the scrambled video data.

[0043] In order to implement the descrambling of the video data scrambled according to the process described in Figure 2, it is the coefficients DC1 which are transmitted as descrambling keys to the descrambling device.

[0044] Preferably, the various coefficients DC1 are transmitted to the descrambling device after having been encrypted by an algorithm with key K. The transmission of the coefficients DC1 is preferably performed in the stream of data which contains the scrambled video data.

[0045] In the case in which the scrambling process implements a process according to Figure 1 and a process according to Figure 2 as mentioned above, a descrambling key consists either of a permutation rank R, or of a coefficient DC1, or of the combination of a permutation rank R and a coefficient DC1.

[0046] Irrespective of the way in which the data have been scrambled, namely a process according to Figure 1, a process according to Figure 2, or else a process according to Figures 1 and 2, the data are descrambled, under the action of descrambling keys, by operations which are the inverse of the operations which served to scramble the data. These inverse operations are performed, for example, by programming a microprocessor.

Claims

1. Process for scrambling video data in the MPEG2 video format, the video data representing at least one block of at least one image coded in INTRA mode (I) and comprising data (AC, DC) arising from a discrete cosine transform operation (DCT) and consisting, for each block, of a first coefficient (DC) representing the mean intensity of the pixels of the block and of coefficients (AC) representing the intensity variations between pixels of the block, characterized in that the scrambling of the video data is carried out by a permutation step, within at least one and the same block, according to a permutation rank (R), of the coefficients (AC1) representing the intensity variations between pixels of the block.

2. Process according to Claim 1, characterized in that the scrambling of the video data comprises a step of substituting a coefficient (DC2) chosen under the action of a command (C) for the coefficient (DC1) representing the mean intensity of the pixels of the block.

3. Process according to Claim 2, characterized in that the command (C) is chosen randomly.

4. Process for descrambling scrambled video data, the descrambling of the video data being performed under the action of a descrambling key, characterized in that the video data are data scrambled according to the process of Claim 1 and in that the descrambling key consists of the rank (R) of the permutation of the coefficients (AC1), representing the intensity variations between pixels of the block.

5. Process for descrambling scrambled video data, the descrambling of the video data being performed under the action of a descrambling key, characterized in that the video data are data scrambled according to the process of Claim 2 or 3 and in that the descrambling key is the coefficient (DC1) representing the mean intensity of the pixels of the block.

6. Device for scrambling video data in the MPEG2 video format, the video data representing at least one block of at least one image coded in INTRA mode (I) and comprising data (AC, DC) arising from a dis-

crete cosine transform operation (DCT) and consisting, for each block, of a first coefficient (DC) representing the mean intensity of the pixels of the block and of coefficients (AC) representing the intensity variations between pixels of the block, characterized in that it comprises means for descrambling the video data under the action of a descrambling key consisting of at least one of the data arising from the operation for processing the data arising from the discrete cosine transform operation (DCT).

7. Decoder of video data coded according to the MPEG2 video standard, comprising a device for descrambling scrambled video data, characterized in that the descrambling device is a device according to Claim 6.

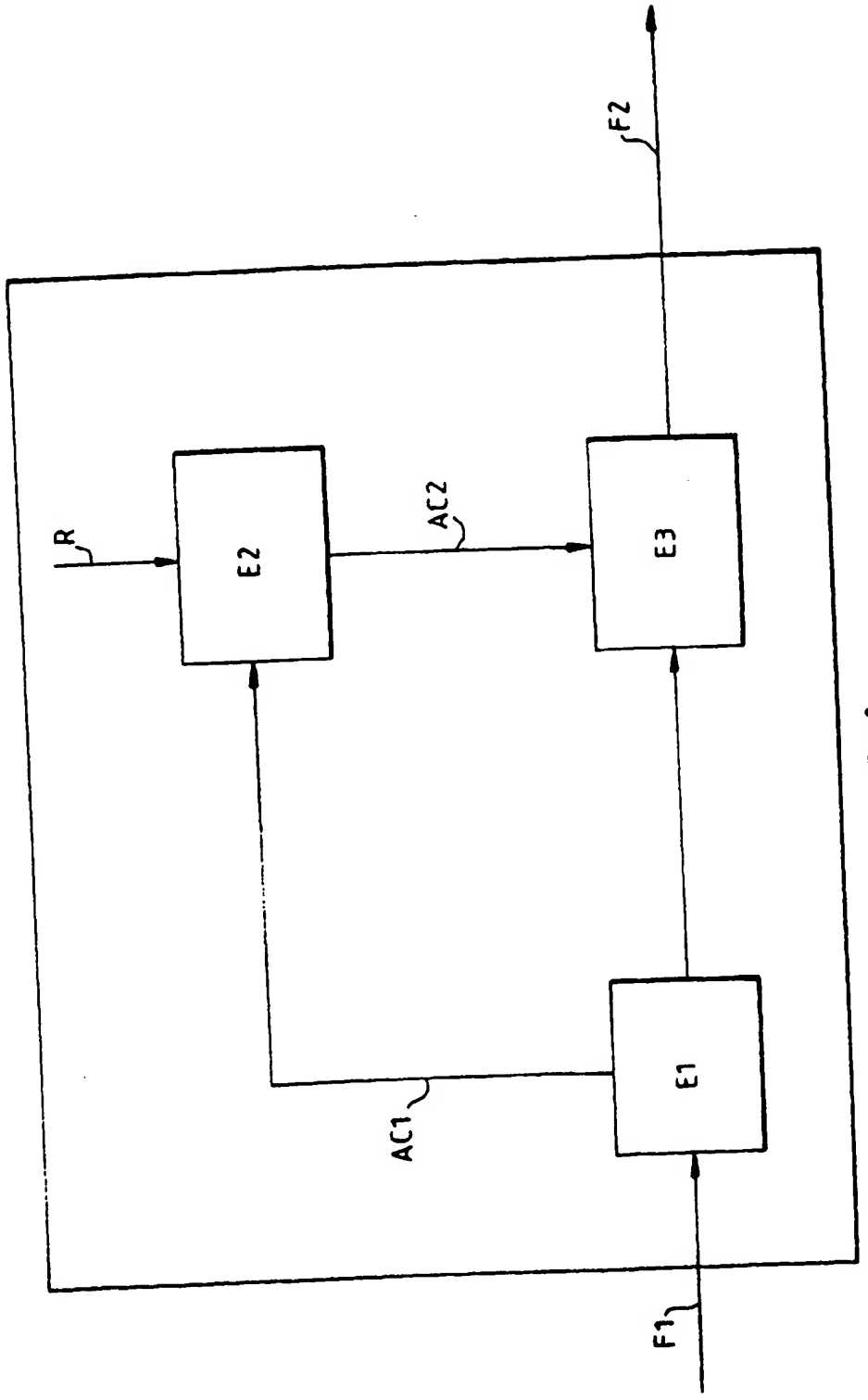

FIG.1

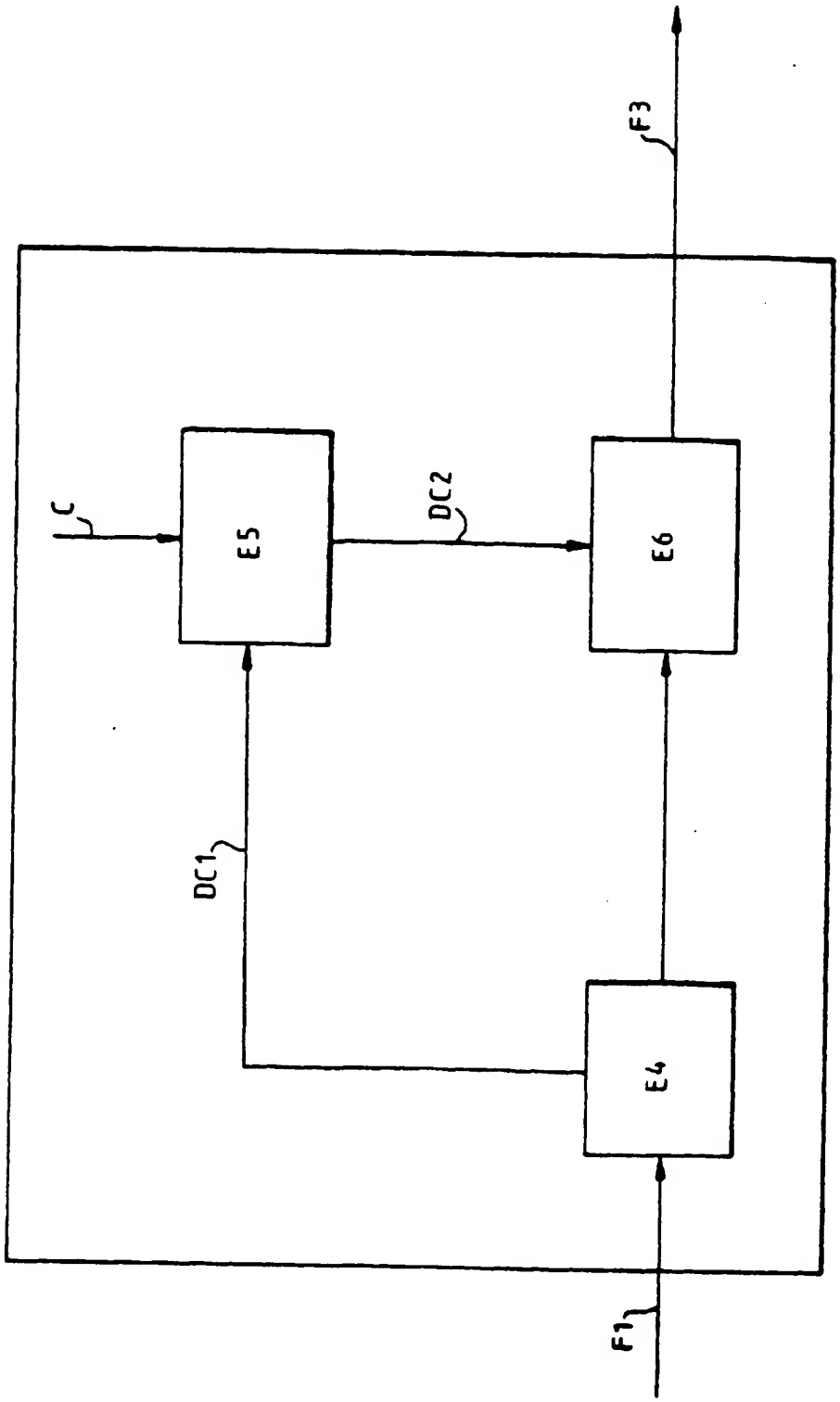

FIG.2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 40 2647

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	HARRICK M VIN ET AL: "EFFICIENT FAILURE RECOVERY IN MULTI-DISK MULTIMEDIA SERVERS" 25TH. INTERNATIONAL SYMPOSIUM ON FAULT TOLERANT COMPUTING DIGEST OF PAPERS, PASADENA, JUNE 27 - 30, 1995, no. SYMP. 25, 27 June 1995, pages 12-21, XP000597773 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS * paragraph 3.1.2 * * figure 3 *	1-7	H04N7/167 H04N7/30
A	EP 0 633 703 A (SONY CORP) 11 January 1995 * abstract * * figures 5-7 * * column 12, line 47 - column 13, line 28 *	1-7	
A	EP 0 619 677 A (MATSUSHITA ELECTRIC IND CO LTD) 12 October 1994 * claims 1,4,5; figure 2 *	1-7	
A	EP 0 359 729 A (TELEVERKET) 21 March 1990 * abstract * * column 3, line 60 - column 4, line 15; figures 2-4 *	1-7	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04N
A	EP 0 648 055 A (MATSUSHITA ELECTRIC IND CO LTD) 12 April 1995 * abstract *	1-7	
A	EP 0 674 441 A (NOKIA TECHNOLOGY GMBH) 27 September 1995 * column 3, line 20 - line 46 *	1-7	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 February 1999	Berbain, F

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 40 2647

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

08-02-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0633703 A	11-01-1995	JP 7030855 A	31-01-1995
		CA 2126946 A	09-01-1995
		US 5535275 A	09-07-1996
EP 0619677 A	12-10-1994	JP 6296279 A	21-10-1994
		JP 6296175 A	21-10-1994
		JP 6303232 A	28-10-1994
		JP 7023367 A	24-01-1995
		JP 7111645 A	25-04-1995
		US 5546461 A	13-08-1996
EP 0359729 A	21-03-1990	SE 503549 C	01-07-1996
		DE 68922166 D	18-05-1995
		DE 68922166 T	10-08-1995
		SE 8803264 A	16-03-1990
		SE 465051 B	15-07-1991
		SE 8903694 A	16-03-1990
EP 0648055 A	12-04-1995	JP 7111646 A	25-04-1995
		JP 7111647 A	25-04-1995
		JP 7336666 A	22-12-1995
		US 5706346 A	06-01-1998
EP 0674441 A	27-09-1995	FI 941315 A	22-09-1995
		DE 69506463 D	21-01-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82